Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 11, No. 2, June 2025, pp. 322-345
ISSN: 2338-3070, DOI: 10.26555/jiteki.v11i2.30815

Quantitative Assessment of Blacklist-Based Malicious Domain Filtering for ISP Security: Balancing Protection and Performance

Muhti Subiyantoro, Mukhammad Andri Setiawan
Master of Informatics, Universitas Islam Indonesia, Jl. Kaliurang KM. 14.5 Sleman Yogyakarta 55584

ARTICLE INFO

Article history:

Received March 24, 2025
Revised June 09, 2025
Accepted June 30, 2025

Keywords:

Malicious Domain Filtering;
ISP Cybersecurity;
Blacklist-Based Security;
Network Performance Metrics;
Perimeter Defense;
Traffic Flow Analysis

ABSTRACT

The growing dependence on internet connectivity has heightened cybersecurity threats through malicious domains that facilitate malware, phishing, and botnet operations. These threats significantly impact individuals and organizations, particularly in Internet Service Provider (ISP) settings. Domain filtering on firewalls is a common defensive strategy, yet its effectiveness remains underestimated in large-scale ISP settings. Previous studies have not focused specifically on security systems commonly employed by ISPs, impeding practical adoption. The research contributions are: (1) developing a cost-effective malicious domain filtering approach specifically designed for ISP environments requiring minimal infrastructure investment, and (2) providing quantitative evidence of how blacklist-based filtering impacts both security effectiveness and network performance. The methodology employs alternating firewall states over four time periods to collect metrics including connection flow, bandwidth utilization, and packet rate. Results demonstrate that malicious domain filtering improves security while causing a 2.49% increase in total connection flow due to retry mechanisms. This process yields a 24.5% reduction in total bytes transferred, 10.5% decrease in packets sent, 22.58% reduction in bandwidth, and 8.81% decrease in packet rate. The study identified 1,919 malicious IP addresses blocked from 1,090 user attempts to access harmful domains. These findings confirm blacklist-based domain filtering strengthens security and enhances bandwidth efficiency by mitigating unwanted traffic. This approach is particularly relevant for ISPs, providing a cost-effective solution that balances cybersecurity with optimized network performance, allowing organizations to protect users while maintaining operational effectiveness.

Corresponding Author:

Muhti Subiyantoro, Islamic University of Indonesia, Jl. Kaliurang KM 14, Sleman, Yogyakarta 55584, Indonesia
Email: 21917014@students.uii.ac.id

1. INTRODUCTION

In the increasingly advanced digital era, the Internet has become an integral element in daily life, supporting various essential aspects such as communication, financial transactions, education, and other activities [1], [2], [3]. However, the development of this technology also brings significant challenges in the form of cybersecurity threats [4], [5], [6]. One of the most significant threats is the use of malicious domains by malicious actors to carry out various cybercriminal activities, such as botnet control, phishing, online fraud, and malware distribution [7], [8], [9].

A malicious domain refers to a domain name designed for malicious purposes by individuals or groups with malicious intent. These domains are often used as infrastructure to launch cyberattacks, redirect unsuspecting users to malicious sites, or steal personal or financial information [10], [11]. The complexity of these threats continues to increase due to the use of sophisticated techniques by actors, such as DNS hijacking, domain shadowing, and dynamic domain exploitation, which significantly complicates detection and mitigation efforts [12].

The existence of malicious domains is a significant concern for cybersecurity professionals and global organizations, given their detrimental impact that can extend to individuals, companies, and national security [13], [14]. For example, phishing attacks based on fake domains have caused significant financial losses, while domains used for malware distribution are capable of infecting millions of devices in a short period [15], [16]. A recent study conducted by Hewlett-Packard revealed that 70% of all internet-connected devices are alarmingly vulnerable to potential attacks [17]. In addition, the increase in international regulations and policies related to cybersecurity and domain management has spurred further research in this area. Governments and global organizations, such as the Internet Corporation for Assigned Names and Numbers (ICANN), continue to work to strengthen the framework for overseeing domain registrations to prevent misuse [18], [19].

In Indonesia, the growth of Internet Service Providers (ISPs) and computer network development have significantly contributed to national digital transformation. According to data from the Central Statistics Agency (BPS), the number of ISPs increased from 331 in 2018 to 828 in 2022. In addition, 66.48% of Indonesia's population now has internet access, with 91.95% of users coming from individual customers. The expansion of the internet network to remote parts of the country creates dynamic challenges as well as excellent opportunities for various groups [20], [14]. One of the dominating global trends is the emergence of the metaverse, which is a collection of immersive and interconnected digital spaces that allow user interaction in computer-generated virtual environments [23], [24], [25].

Responsibility for cybersecurity is now a shared responsibility between internet users and ISPs. Cyber resilience involves many stakeholders, including individuals, organizations, governments, and insurance companies. However, at the ISP level, especially in the growing ones, financial constraints are a significant obstacle to providing complex customer protection. According to a survey from the Indonesian Internet Service Providers Association (APJII) in 2022, as many as 70.12% of small, micro, and medium enterprises (MSMEs) and corporations have not had adequate cyber-attack mitigation measures. The main barriers to building a firewall system include high application costs, licenses, and hardware investments. Therefore, a more efficient and affordable security strategy is needed to increase national cyber resilience. In addition, many ISPs still face challenges in terms of human resources and competencies that are not entirely by the needs of cybersecurity management [21]-[24]. The strategy of securing customers through perimeter security services to reduce the chances of cybercrime has become a necessity that cannot be postponed anymore [25], [26], [27].

This research aims to make an economic contribution and offer a solution in the form of a simple firewall to ISPs to filter malicious domains using existing infrastructure without requiring high costs. This solution is designed as a form of ISP responsibility to protect customers from cyber threats. In addition, the study is also expected to provide practical recommendations for cybersecurity professionals and policy guidance that organizations can adopt to strengthen defenses against malicious domain threats. The proposed approach is designed to remain technically complex but flexible so that it can be applied in a variety of system environments.

The main question that guides this study is: *"How effective are malicious domain filtering techniques in improving network security through firewall perimeter services?"* This research takes an approach according to the identification and filtering of malicious domain names in internet activity. This technique is considered an effective method to protect users from cyber threats. Malicious domains that have been identified are collected in the form of blacklists, which then become one of the key components of protection in enterprise security systems.

Several studies have examined the intersection of artificial intelligence and cybersecurity threats. [28] provided a comprehensive framework analyzing AI's dual role in cybersecurity, demonstrating how artificial intelligence both enables sophisticated cyber attacks through automated social engineering and intelligent malware generation while simultaneously empowering advanced defense mechanisms via threat situational awareness and automatic vulnerability detection. However, existing research predominantly focuses on conceptual frameworks and broad AI applications without addressing the specific operational challenges faced by Internet Service Providers (ISPs) in implementing quantifiable security measures. While these studies offer valuable theoretical insights into AI-enabled cyber threats, they lack the empirical validation and performance benchmarking necessary for practical ISP-level security implementations. This research gap highlights the need for quantitative assessment methodologies that can evaluate the effectiveness of specific security mechanisms, such as blacklist-based domain filtering, while considering the critical balance between protection capabilities and network performance in real ISP operational environments. In the domain of malicious domain detection, [29] developed a comprehensive DNS dataset comprising approximately 90,000 domain names with 34 extracted features for supervised machine learning classification of malicious and non-malicious domains. Their research contributed significantly by creating a balanced dataset that combines DNS logs with Open Source Intelligence (OSINT) data enrichment processes, incorporating features such as domain entropy,

creation dates, IP reputation, and geolocation information to enable automated detection of previously unknown malicious domains beyond traditional blacklist approaches. However, their work primarily focuses on feature extraction and dataset creation for machine learning model development without addressing the practical implementation challenges faced by ISPs in operational environments. While Marques et al. provide valuable insights into domain characteristics that can distinguish malicious from benign domains, their research lacks quantitative assessment of real-world filtering performance, cost-benefit analysis of protection versus network performance trade-offs, and evaluation of blacklist effectiveness in actual ISP infrastructure deployments. This gap highlights the need for empirical studies that translate machine learning capabilities into measurable security improvements while considering the operational constraints and performance requirements that ISPs must balance in their network security implementations.

The research [30] develops and describes the security architecture of the Network Security Centre (NSC) in the context of a modern intranet. The main focus is to create a practical Information Security (IS) maintenance system to protect IS objects in corporate networks from computer attacks. The study offers a structural model for an intranet that includes NSC, which integrates various resources (organizational, software, hardware, and human) to detect and respond to IS incidents in real-time. The research emphasizes the importance of using firewalls, especially Next-Generation Firewalls (NGFWs), as part of perimeter protection tools and internal network infrastructure. Firewalls function to control access and protect the network from external threats. The study [31] developed a classification method to identify potentially malicious domain names using cardinality analysis. This method is expected to increase the effectiveness of blacklists used to block harmful internet activities, such as spam and phishing, in a more automated and efficient way compared to the current public blacklists. The study offers a classification method that uses cardinality analysis to identify access patterns from multiple clients to various domain names. In addition, it leverages large DNS query-response data (26 million data points) to test and develop classification models. This includes analyzing the frequency of access and response patterns of domain names to determine whether they are malicious. Overall, the study made a significant contribution to the development of more efficient methods for managing and maintaining malicious domain blacklists, which is crucial in improving cybersecurity.

While previous studies have provided valuable insights into AI-enabled cybersecurity frameworks, sophisticated detection algorithms, and feature-rich datasets for machine learning-based domain classification, they largely overlook the critical operational challenges ISPs face in deploying and evaluating these systems in real-world settings. These works primarily focus on either conceptual models or data-driven approaches without quantifying the trade-offs between security effectiveness and network performance in ISP environments. Thus, a significant research gap remains in the empirical validation and practical implementation of blacklist-based malicious domain filtering solutions, specifically concerning the balance between robust protection and acceptable performance impacts for ISPs. My research directly addresses this gap by providing a quantitative assessment of blacklist-based filtering in ISP security environments, aiming to deliver actionable insights for optimizing protection mechanisms while minimizing operational overhead.

2. METHODS

This research was conducted through direct experiments on ISP networks. Fig. 1 The research methodology encompasses four primary phases: System Identification for comprehensive characterization of the target network system, System Requirements Analysis to establish functional specifications and security policies, Design and Implementation of the experimental framework with monitoring infrastructure, and Live Experiment Setup for real-time experimental environment deployment. The live experimentation phase involves four alternating periods with systematic Firewall Filter ON/OFF cycles, implementing continuous data collection across six critical network performance metrics including BPS (Bytes Per Second), PPS (Packets Per Second), BPP (Bytes Per Packet), Total Flows, Total Bytes, and Total Packets, while utilizing network infrastructure components comprising Customer Networks, Distribution Router, Traffic Flow Collector, and Internet Gateway. The analysis phase consists of comprehensive Data Analysis through statistical evaluation and performance comparison, Evaluation of firewall effectiveness and security impact assessment, and Implementation Recommendations providing evidence-based optimization guidelines. This flowchart represents a systematic live experimentation methodology designed to evaluate firewall filter effectiveness in authentic network environments through comprehensive measurement protocols, enabling empirical assessment of security-performance trade-offs and providing actionable insights for network security optimization in production environments.

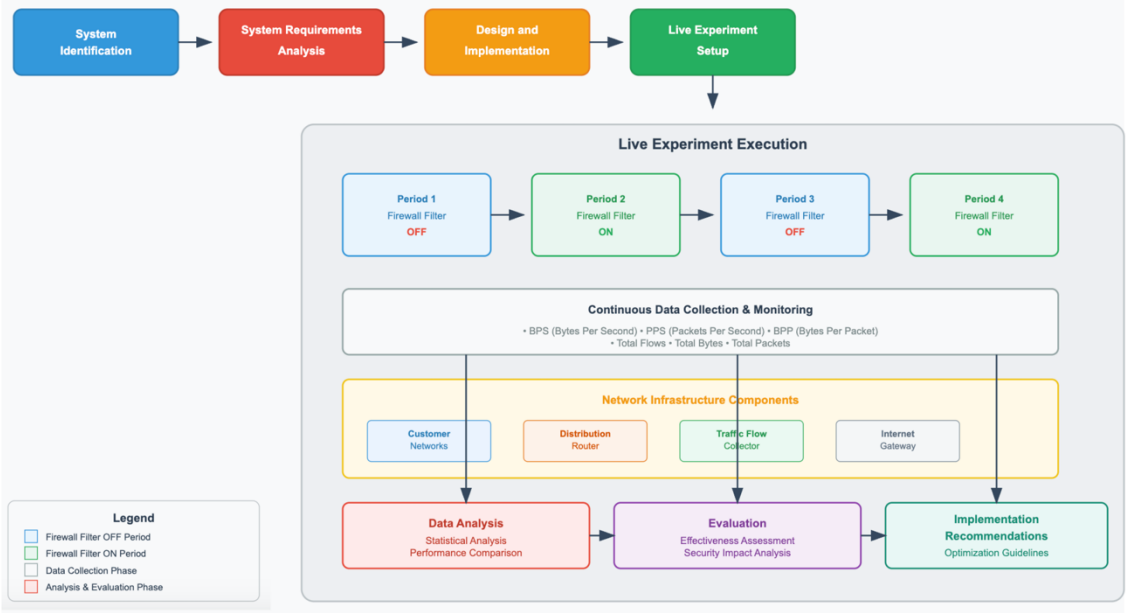

Fig. 1. Flow of The Research Experimental Methode

2.1. System Identification

The first stage in this study is identifying ISP systems and infrastructure that are the objects of research. Identify research objectives in the following aspects:

a. The direction of the focus of ISP research and technology
   ISPs selected as research objects must have a research focus that is relevant to the topic of cybersecurity. This ISP has not implemented a firewall system specifically designed to protect customers from cyber threats [32]-[35].
b. Operational and Infrastructure Scale
   The ISP that is the object of the study has a broad operational scale, is supported by Fiber Optic and Wireless infrastructure, and uses multi-homing Border Gateway Protocol (BGP) for upstream connections. This infrastructure is considered relevant to support the planned scale of research.
c. Data access permissions
   The selection of ISPs also considers the ability to provide legal access to data or network logs and follow privacy regulations. In this case, the researcher is a consultant team member who has obtained official permission to research the ISP network [36], [37].

In addition to system identification, a physical survey is also carried out to understand the hardware used at the ISP. The survey results show that ISPs use:

- MikroTik Router,
- Server with Linux operating system,
- Optical Line Terminal (OLT),
- Optical Network Terminal (ONT),
- Wireless Point-to-Point, dan
- Wireless Point-to-Multi-Point.

These devices have interfaces in the form of Ethernet and fiber optic Small Form-Factor Pluggable (SFP), which will later be relevant to the design and compatibility of the system to be designed.

The use of blacklists to block malicious domains in firewalls remains very relevant today as the main layer of defense in network security. With the increasing number of cyber threats such as phishing, malware, and Command-and-Control (C2) servers, blacklists allow organizations to proactively block access to domains that have been known to be malicious [38], [39]. Although this method has limitations in dealing with new threats (zero-day threats), the integration of blacklists with constantly updated threat intelligence helps improve its effectiveness. Studies by [40], [41] show that the use of blacklists integrated with other security solutions, such as DNS filtering and Intrusion Prevention Systems (IPS), can significantly reduce the risk of attacks. This approach remains an integral part of a layered security strategy.

The next stage is the collection of malicious domain data from various trusted sources, such as threat intelligence feeds, public databases, and forensic search results. The data sources used include domains known to be involved in malicious activity, both newly detected. One of the primary references used is data from Polska's CERT, Poland's first incident response team under the auspices of the NASK (Scientific and Academic Computer Network), a scientific research institute [42]. Complete information can be accessed through their official website, https://cert.pl. Polska CERT focuses its research on collecting, verifying, and validating malicious domain data from various sources worldwide. Domains classified as malicious are typically involved in activities such as:

- Botnet control,
- Fake online investments,
- Fake email attachments,
- Fast fund transfer requests,
- Fake online stores,
- Phishing in online games,
- Online gambling sites, and so on.

The malicious domain data collected by CERT Polska is available in a format that is compatible for use on various network device platforms, including routers. This format allows such data to be integrated as part of firewall attributes to improve network security. This information can be accessed openly, updated every 5 minutes, and used by anyone who needs it, making it one of the important data sources in this study.

2.2. System Requirements Analysis

DNS queries have drawn the attention of Internet Service Providers (ISPs) who utilize them to gain deeper insights into their customer base. Meanwhile, malicious actors launch attacks aimed at manipulating DNS information to redirect users toward harmful content. The DNS infrastructure continuously faces denial-of-service attacks that pose threats to its operational availability. Paradoxically, the widespread success of DNS makes it an appealing tool for cybercriminals, who inadvertently exploit it to facilitate, coordinate, and enhance their attacks, such as steering end-users toward malicious websites [43]. Referring to the previous identification, an analysis of system needs was carried out to design and develop an address list-based filtering mechanism by utilizing the domain data that had been collected. The system is designed to use address lists as network traffic detection parameters, which will then be included in the category of malicious domains. The main functions of the router are to block requests to malicious domains that have been registered, log the source and destination IPs, and monitor the traffic flow, which is then stored in the collector machine.

From the literature study on ISPs, the types of traffic flow in line with the parameters of source address (src-addr) and destination address (dst-addr) can be categorized as follows:

- Traffic from Client to Router (Upload – Request Client to Router)
- Traffic from Router to Client (Download – Response Router to Client)
- Traffic from Router to the Internet (Upload – Request Router to the Internet)
- Traffic from the Internet to Router (Download – Response from the Internet to Router)
- Traffic from Client to Internet (Upload – Request Client to Internet)
- Traffic from the Internet to Client (Download – Response from the Internet to Client)

In addition, communication traffic on the Domain Name System (DNS) is divided into two categories:

- DNS Request: A request from the Client to the DNS Server.
- DNS Response: A reply from the DNS Server to the Client.

Fig. 2 illustrates the DNS resolution process and web access within a computer network. As an example, it begins with a client wanting to access www.example.com. The communication process occurs in four main stages: first, the client sends a request "What is the IP of www.example.com?" to the router with DNS cache; second, the router forwards the request to the DNS server if the information is not available in the cache; third, after the IP address (x.x.x.x) is obtained by the router, it is stored in the cache and forwarded back to the client, then the client sends an HTTP/HTTPS request directly to that IP address which is the web server where www.example.com is hosted; and finally, the web server with IP x.x.x.x provides a response back to the client, completing the communication process that underlies virtually all web browsing or domain interactions in modern networks.

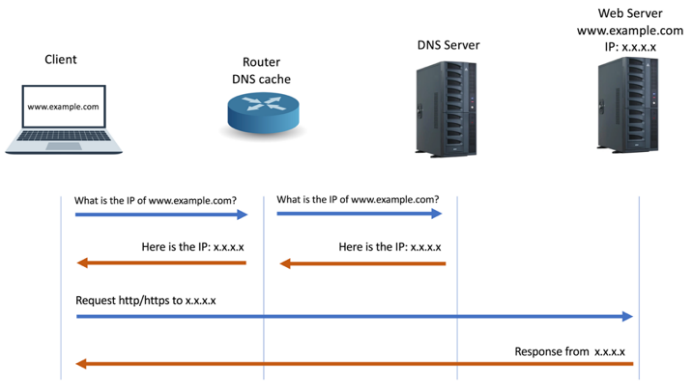

Fig. 2. Client Traffic Domain Request Communication

Reliant on this communication mechanism, the firewall is designed to drop client request traffic to IPs registered on the malicious domain blacklist. The file containing the address list of malicious domains in .rsc format is imported into the Router and integrated through the address-list menu. Filter firewalls are applied to direct traffic from the Client to the IP Domain that is identified as malicious. The traffic collected is the traffic on the capture interface on the router that leads to the Client network. The router sends all the captured traffic data to the collector server using the TCP protocol on port 2556. The research also utilizes the Traffic Flow feature on the MikroTik Router, which allows the reading of network traffic passing through the router's interface. The data from these readings can be passed to a Linux-based server as a collector. The NFDUMP open-source application is used on a collector server, which works to:

- Accommodates the catch from the Traffic Flow via TCP protocol on port 2556.
- Analyze the collected traffic data.

The selection of MikroTik routers for this study was based on their prevalence in small to medium ISP deployments in Indonesia, their robust filtering capabilities, and their compatibility with standard blacklist formats. Similarly, NFDUMP was chosen for traffic analysis due to its ability to efficiently process large volumes of network data, its compatibility with NetFlow data formats, and its extensive filtering and aggregation capabilities that enable detailed statistical analysis. These tools together provide a cost-effective yet powerful framework for implementing and evaluating malicious domain filtering in production ISP environments. With this integration, traffic flow analysis can be carried out more in-depth to identify malicious patterns and activities, allowing the system to proactively protect the network from malicious domain threats.

2.3. Design and Implementation

This stage aims to build a prototype of the filtering system and test its effectiveness in both simulated and real network environments. Testing is carried out to ensure the system can accurately recognize malicious domains registered in the blacklist, as well as to evaluate the performance of the system in line with several parameters, including [44]:

- True Positive Rate (TPR) – The correct detection level of malicious domains.
- False Positive Rate (FPR) – The rate at which non-malicious domain detection errors are made.
- Number of Traffic Captured – The volume of traffic data that was successfully recorded.
- Firewall Function – The ability of a firewall to block access to malicious domains.

Fig. 3 shows an illustrates the network traffic data collection system architecture (NetFlow) consisting of several strategic components: Customer networks (Customer 1, 2, through n) are connected to a Distribution Router that serves as the traffic aggregation point, while the Main Router functions as both Traffic Flow Capturer and Traffic Flow Sender connecting the local network to the Internet. Network traffic data (Traffic Flow Object) is collected from the interface between both routers and transmitted to the Traffic Flow Collector which serves as the data storage and processing server. This system enables comprehensive monitoring and analysis of network traffic patterns from various user segments, providing visibility for security purposes, performance optimization, and digital forensics from the obtained nfcapd files.

NFDUMP, an open-source software, is used on the Traffic Flow Collector server to collect network traffic data. The command line in nfdump can be used to filter the output of a flow file record with the format nfcapd [45], [46]. The traffic sent by the MikroTik router will be stored in a binary file format named nscapd. YYYYMMDDhhmm, which is generated every five minutes. Fig. 4 illustrates the network data processing workflow using the nfdump utility. The binary input files named nfcapd.2023xxxx are network capture files

from the research data folder. These files are processed using specific parameters to read the data. The nfdump process then applies specific filters to identify TCP connections. The processing output can be in two formats: text format that generates structured reports, or binary format that produces new binary files with similar names nfcapd.2023xx. With this approach, the system can efficiently record and analyze traffic flow data, enabling informed decision-making based on observed traffic patterns. The results of the analysis not only support prototype testing but also serve as a basis for evaluating the effectiveness of the system in detecting and mitigating malicious domain threats.

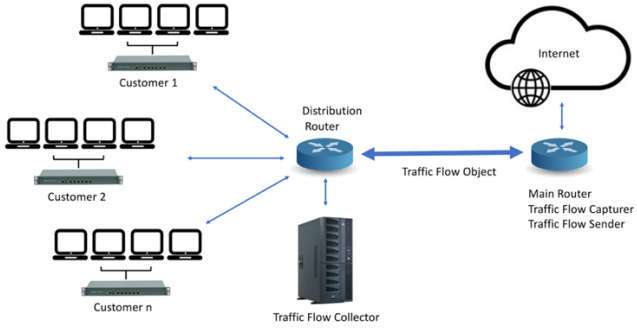

Fig. 3. Research Diagram Prototype

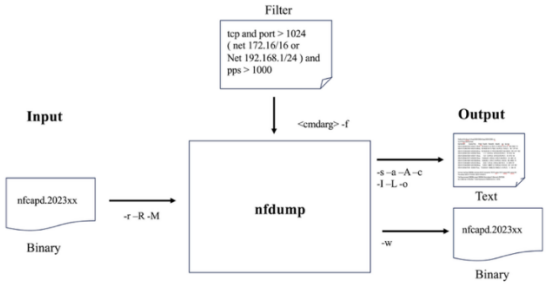

Fig. 4. NFDUMP as a collector and analyzer software

In this section, experiments are conducted to simulate the mechanism based on the partially planned workflow. The first step involves retrieving, modifying, and testing the address-list file, which ensures that the router can accept the address-list file script format and recognize the IP addresses of malicious domains registered in the database. The second step focuses on implementing and verifying the blocking function against the list of IP addresses identified as malicious domains, ensuring that the router operates effectively.

In the third step, the router is set up as a catching system, capable of reading the traffic flowing on the detected path. The router also serves as a sender to transmit the data capture to the collector, where the data will be stored. The final design that has been simulated is deployed on the ISP production machine, with the blacklist integrated using the address-list feature on the Traffic Flow Capturer & Sender Router.

To ensure statistical validity of our findings, we collected data over four distinct time periods, alternating between firewall-ON and firewall-OFF states, each period lasting nine days. This approach allowed us to temporal variations in network traffic and user behavior. We calculated confidence intervals for all key metrics (95% CI) and performed statistical significance testing ($p < 0.05$) to validate that observed differences between firewall states were not due to random variation [17]. Potential confounding factors, such as changes in user behavior or external network conditions, were monitored throughout the study period.

Next, the firewall settings are configured to drop all client request packets whose destination addresses are included in the blacklist, as well as log the IP addresses of the local area network (LAN) that make requests. The traffic capture process is conducted continuously for 24 hours every day for two weeks at each experimental stage. The first stage captures traffic when the firewall is enabled (ON), while the second stage records traffic when the firewall is disabled (OFF). The third stage captures traffic with the firewall enabled (ON), followed by the fourth stage, which captures traffic when the firewall is disabled (OFF). Observations are made periodically to ensure the data is stored in the collector as expected. Given the volume of data

generated, special attention is devoted to ensuring that the hard disk drive (HDD) has sufficient space to accommodate the data.

2.4. Analysis and Evaluation

This stage aims to analyze the test results to assess the effectiveness of the method that has been developed. The analysis compares the results of network traffic when the firewall is activated and when the firewall is disabled. This comparison aims to measure the system's improved network protection. All blocked IP addresses and those requesting malicious domains are recorded in detail during this process. The results of the evaluation include:

- The number of domains successfully detected and blocked.
- The system's success rate in identifying malicious domains without impacting network performance.
- The effectiveness of firewalls in preventing access to malicious domains is based on the number of successfully terminated requests.

2.5. Implementation Recommendations

According to the research results, practical recommendations are prepared for implementation in the network security system. This recommendation is designed to support organizations in determining a firewall strategy that follows the principle of simplicity without sacrificing complexity. The goal is to guide in choosing the right firewall strategy grounded on specific needs, such as:

- Utilize domain-based blacklist address lists to prevent access to malicious domains.
- Integrate the filtering system into the existing infrastructure without requiring large investments.
- Balancing system efficiency and complexity to be adaptable to various network environment scenarios.

3. RESULTS AND DISCUSSION

Research that includes planning, simulation, and implementation shows that the system is running well without disrupting ISP operations. The supporting data produced during the research process, from the beginning to the end, is sufficient for further analysis.

3.1. Malicious Domain Address List

The address list format used is adjusted to the router device operated by the ISP, in this case, the MikroTik router. Therefore, the chosen address list format is blacklisted with the .rsc file extension. An analysis of the various file formats available found that the .rsc file has minimal content, while the .csv file contains much more complete data. As of the end of 2022, Table 1 shows that 84,765 malicious domains were recorded in a .csv file. Given the limitations of the .rsc file format, it was necessary to modify and convert the data from the .csv format to .rsc to meet the needs of firewall implementation on MikroTik routers. This conversion process ensures that the entire list of malicious domains can be integrated into the system in a compatible format without losing important data [47], [48]. In doing so, the integrity of the information is preserved, and the firewall is better equipped to protect against these threats [42], [43].

Fig. 5 is the result of converting a .csv file containing a list of malicious domains into a .rsc format, which is used for MikroTik router configurations. The .rsc file includes commands to add each domain to the firewall's address list under the label MALICIOUS_DOMAIN. By importing this file into MikroTik routers, administrators can easily integrate and apply the list of identified malicious domains, enhancing the router's security by blocking or restricting access to these threats.

Table 1. Last of 10 from the 84,765 malicious domain address list .csv file

No	Domain Address	Date of Entry
84756	balender3d.com	2022-12-31T07:38:55
84757	profisthebitsera-po.fababeok.com	2022-12-31T07:54:22
84758	inpost-pl-hid226ks.antenaj3.xyz	2022-12-31T13:00:19
84759	netflspl.com	2022-12-31T13:45:02
84760	profisthebitsera-po.betulaup.com	2022-12-31T15:33:59
84761	auth-web-apps.com	2022-12-31T15:38:22
84762	zz3v1x.webwave.dev	2022-12-31T15:47:46
84763	dicsord-snows.com	2022-12-31T17:59:27
84764	my-diya-inc.com	2022-12-31T20:14:59
84765	profisthebitsera-po.biferyal.com	2022-12-31T21:55:51

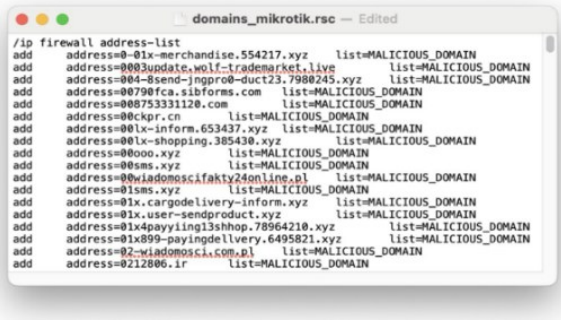

Fig. 5. Result address list .rsc conversion from .csv file

3.2. Malicious Domain IP Traffic

At the beginning of data collection, traffic requests from the client's source address to the malicious domain and inbound traffic from the malicious domain to the client's local address were evaluated. During the first two weeks, observations were made on the traffic. Table 2 refers to the logs recorded in the firewall list, 1,090 client IP addresses made requests to malicious domains, and 1,919 inbound IP addresses from malicious domains.

Table 2. The last 10 lists from 1090 IP client requests to the malicious domain

```
#jan /25/2023  9:15:53 by RouterOS 6.49.6
#software id = PVT6-1QVA
#
Flags    : X - disabled, D - dynamic
 1081    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.15.81
         creation-time=jan/24/2023 23:41:51

 1082    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.13.88
         creation-time=jan/25/2023 00:16:19

 1083    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.26.110
         creation-time=jan/25/2023 01:38:35

 1084    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.26.115
         creation-time=jan/25/2023 04:29:27

 1085    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.27.240
         creation-time=jan/25/2023 07:27:24

 1086    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.26.121
         creation-time=jan/25/2023 07:58:44

 1087    D list=REQUEST_MALICIOUS-DOMAIN address=10.116.216.22
         creation-time=jan/25/2023 08:02:06

 1088    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.15.104
         creation-time=jan/25/2023 08:47:22

 1089    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.26.47
         creation-time=jan/25/2023 09:02:04

 1090    D list=REQUEST_MALICIOUS-DOMAIN address=192.168.15.109
         creation-time=jan/25/2023 09:15:16
```

Table 3 is extracted from a firewall log, which records traffic flow data showing attempts by inbound connections from malicious domains targeting the local network. The table displayed lists the last 10 entries, specifically from entry numbers 1910 to 1919, where each entry represents a dynamic firewall rule automatically created to block inbound connections from various suspicious IP addresses. These logs include critical information such as the timestamp of each entry, IP addresses of the detected malicious domains, and the unique identifiers for each record. This helps in identifying and mitigating threats from inbound malicious domains efficiently.

Table 3. The last 10 lists from 1919 IP client requests to the malicious domain

```
# jan /25/2023  9:16:55 by RouterOS 6.49.6
# software id = PVT6-1QVA
#
Flags    : X - disabled, D - dynamic
 1910    D list=INBOUND_MALICIOUS-DOMAIN address=18.67.111.7
         creation-time=jan/25/2023 00:14:13

 1911    D list=INBOUND_MALICIOUS-DOMAIN address=18.67.111.35
         creation-time=jan/25/2023 00:24:45

 1912    D list=INBOUND_MALICIOUS-DOMAIN address=18.67.111.77
         creation-time=jan/25/2023 00:31:22

 1913    D list=INBOUND_MALICIOUS-DOMAIN address=18.67.111.100
         creation-time=jan/25/2023 00:31:22

 1914    D list=INBOUND_MALICIOUS-DOMAIN address=13.227.74.103
         creation-time=jan/25/2023 00:47:53

 1915    D list=INBOUND_MALICIOUS-DOMAIN address=104.21.65.107
         creation-time=jan/25/2023 01:11:42

 1916    D list=INBOUND_MALICIOUS-DOMAIN address=13.225.95.77
         creation-time=jan/25/2023 01:24:56

 1917    D list=INBOUND_MALICIOUS-DOMAIN address=13.225.95.127
         creation-time=jan/25/2023 03:26:07

 1918    D list=INBOUND_MALICIOUS-DOMAIN address=13.33.88.12
         creation-time=jan/25/2023 04:03:03

 1919    D list=INBOUND_MALICIOUS-DOMAIN address=13.227.74.66
         creation-time=jan/25/2023 09:11:45
```

3.3. Trafic Flow Data Analisys

From the data collection stage using the collector server, 199.21 GB of data was obtained, which was stored in 12,351 files. Each file records traffic capture for 5 minutes. From the total data, four sample groups were taken for analysis, each representing nine days:

- First period: The firewall filter is in the OFF state.
- Second period: The firewall filter is in the ON state.
- Third period: The firewall filter is in the OFF state.
- Fourth period: The firewall filter is in the ON state.

The files in the collector are stored in binary format with the name nfcapd. YYYYMMDDhhmm, and the size of each file varies. An example of an analysis command to display Total Flows, Total Bytes, Total Packets, Avg bps, Avg pps, and Avg bpp on January 14, 2023, is as follows:

```
nfdump -R nfcapd.202301140000:nfcapd.202301142355 -s ip
```

Fig. 6 shows a file sample in a directory named DATA_PENELITIAN containing multiple files with the prefix nfcapd followed by timestamps, representing data files generated by the NetFlow Collector server. Each file stores network flow data for a specific time interval on March 28, 2023, with file sizes ranging from around 11 MB to 55 MB. This organized structure allows researchers or network administrators to analyze the captured network traffic data in detail, monitoring traffic patterns and potentially identifying anomalies or security incidents [49].

Table 4 Shows daily data for the period from January 11 to January 25, 2023 (PERIOD I - FILTER OFF), including daily total flows, daily total bytes (in gigabytes), daily total packets (in gigabytes), daily average bits per second (bps) in megabits, daily average packets per second (pps), and daily average bytes per packet (bpp). It highlights fluctuations in network traffic activity between January 14 and January 22, with notable variations in daily average bps and pps, reflecting different traffic patterns for each day.

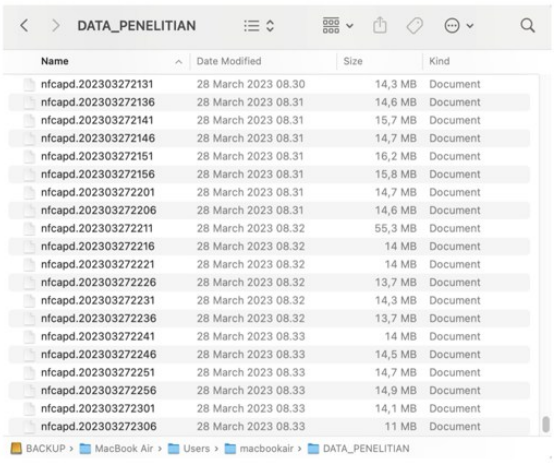

Fig. 6. Data nfcapd file from Collector Server

Table 4. Period I daily data of 9 days - FILTER OF

No	PERIOD I - FILTER OFF11 Jan - 25 Jan '23	DAILY Total Flows	DAILY Total Bytes (G)	DAILY Total Packets (G)	DAILY Avg bps (M)	DAILY Avg pps	DAILY Avg bpp
1	14-Jan	60716624	859,000	1,000	78,000	11426,000	853,000
2	15-Jan	57732688	683,900	0,803	62,100	9114,000	851,000
3	16-Jan	67616336	955,200	1,100	86,700	12762,000	846,000
4	17-Jan	66751328	797,100	0,948	72,300	10747,000	841,000
5	18-Jan	60318768	838,800	0,986	55,900	8213,000	850,000
6	19-Jan	63935200	939,600	1,100	85,300	12670,000	841,000
7	20-Jan	61572992	862,400	1,000	78,200	11431,000	855,000
8	21-Jan	64138704	872,000	1,000	78,900	11687,000	844,000
9	22-Jan	55982864	643,900	0,761	58,500	8635,000	846,000

Table 5 Presents daily data for the period from February 3 to February 12, 2023 (PERIOD II - FILTER ON). It includes daily total flows, daily total bytes (in gigabytes), daily total packets (in gigabytes), daily average bits per second (bps) in megabits, daily average packets per second (pps), and daily average bytes per packet (bpp). The data highlights fluctuations in network traffic activity, showcasing the variations in daily average bps and pps throughout the period, reflecting different patterns of data flow and network usage for each day.

Table 5. Period II daily data of 9 days - FILTER ON

	PERIODE II - FILTER ON3 Feb - 12 Feb '23	DAILY Total Flows	DAILY Total Bytes (G)	DAILY Total Packets (G)	DAILY Avg bps (M)	DAILY Avg pps	DAILY Avg bpp
10	03-Feb	74730912	773,500	1,200	70,200	13556,000	647,000
11	04-Feb	80766400	890,700	1,200	80,800	13715,000	736,000
12	05-Feb	76764672	763,800	1,100	69,400	12142,000	714,000
13	06-Feb	82242384	860,900	1,200	78,100	13639,000	716,000
14	07-Feb	77254992	707,900	1,100	64,200	12135,000	661,000
15	08-Feb	79376176	837,200	1,200	75,900	13695,000	693,000
16	09-Feb	79823323	876,100	1,300	79,500	14438,000	688,000
17	10-Feb	72858844	843,500	1,200	76,900	14046,000	684,000
18	11-Feb	59037903	855,700	1,300	77,500	14451,000	670,000

Table 6 Presents daily network traffic data from February 22 to March 6, 2023, under the condition "FILTER OFF." The recorded metrics include daily total flows, daily total bytes (in gigabytes), daily total packets (in gigabytes), daily average bits per second (in megabits), daily average packets per second, and daily average bytes per packet. The data highlights fluctuations in these metrics, showing peak values on certain

days, indicating varying levels of network activity and data flow, likely corresponding to different patterns of data usage and traffic within the network during this period.

Table 6. Period III daily data of 9 days - FILTER OFF

	PERIODE III - FILTER OFF22 Feb - 6 Mar '23	DAILY Total Flows	DAILY Total Bytes (G)	DAILY Total Packets (G)	DAILY Avg bps (M)	DAILY Avg pps	DAILY Avg bpp
19	23-Feb	60277152	933,000	1,400	84,600	16148,000	655,000
20	24-Feb	58886320	904,100	1,500	82,000	16602,000	617,000
21	25-Feb	57878688	900,100	1,500	81,700	16671,000	612,000
22	26-Feb	58573056	793,200	1,300	71,900	15167,000	592,000
23	27-Feb	60715168	882,200	1,400	80,000	15403,000	649,000
24	28-Feb	64275680	962,400	1,400	87,300	16391,000	666,000
25	01-Mar	65456144	906,000	1,400	82,200	15580,000	659,000
26	02-Mar	57725264	754,200	1,300	68,400	14753,000	579,000
27	03-Mar	54834154	568,600	1,200	51,600	13113,000	491,000

Table 7 Daily network traffic data from March 6 to March 17, 2023, during which a filter was applied ("FILTER ON"). It includes details such as daily total flows, daily total bytes (in gigabytes), daily total packets (in gigabytes), daily average bits per second (in megabits), daily average packets per second, and daily average bytes per packet. The data shows moderate fluctuations in network traffic with a noticeable peak on March 11, suggesting an increased level of data transmission and usage on that particular day, which is consistent with dynamic data patterns within the filtered network.

Table 7. Period IV daily data 9 days - FILTER ON

	PERIODE IV - FILTER ON6 Mar - 17 Mar '23	DAILY Total Flows	DAILY Total Bytes (G)	DAILY Total Packets (G)	DAILY Avg bps (M)	DAILY Avg pps	DAILY Avg bpp
28	06-Mar	61738320	587,000	1,100	53,300	12526,000	532,000
29	09-Mar	48862832	574,100	1,000	52,100	11842,000	550,000
30	10-Mar	47089168	567,700	0,980	51,600	11132,000	579,000
31	11-Mar	46614128	601,700	1,000	54,600	11555,000	590,000
32	12-Mar	45930624	481,700	0,859	43,700	9746,000	560,000
33	13-Mar	47556448	486,800	0,902	44,200	10228,000	539,000
34	14-Mar	42094480	453,400	0,784	41,100	8889,000	578,000
35	15-Mar	50017408	428,300	0,799	38,900	9067,000	536,000
36	16-Mar	52654560	503,300	0,931	45,700	10562,000	540,000

The table above shows fluctuations in Total Flows, Total Bytes, and other parameters referring to the condition of the filter firewall. Further analysis was carried out to see the tendency of the change between the firewall in the OFF and ON conditions, which is presented in the graphical visualization (Figure 8-10).

Fig. **7** The chart displays "DAILY total FLOWS" data over 38 periods, revealing four distinct operational phases separated by complete data cutoffs at points 10, 20, and 30. During periods 1 (days 1-9) and 3 (days 21-29) when the firewall filter was OFF, flows remained relatively stable at 55-65 million units. However, when the firewall filter was activated during period 2 (days 11-19), flows increased significantly by approximately 25% to peak levels of 75-80 million, likely due to enhanced connection tracking generating additional flow records. Conversely, period 4 (days 31-38) with firewall ON showed the opposite effect, with flows dropping to the lowest levels of 45-50 million units, representing a 20% decrease compared to period 3. This contrasting behavior suggests that firewall impact varies depending on network conditions and traffic patterns, with the overall trend showing a gradual decline in total flows over time, indicating either network optimization, configuration changes, or evolving traffic characteristics that affect firewall performance differently under varying operational conditions [50].

Fig. 8 The "DAILY TOTAL BYTES (G)" chart displays data volume in gigabytes over 38 periods with similar phase divisions as the previous graph, including complete data cutoffs at points 10, 20, and 30. During periods 1 (days 1-9) and 3 (days 21-29) with firewall filter OFF, data volumes ranged between 800,000-950,000 GB, while firewall activation showed contrasting effects across different periods. In period 2 (days 11-19) with firewall ON, volumes remained relatively stable around 800,000 GB, representing only a 5-10% decrease compared to period 1, contrasting with the flow increase observed in the previous chart. However, period 4 (days 31-39) with the firewall activated showed a dramatic 40% reduction to 400,000-600,000 GB compared to period 3. This pattern demonstrates that while firewall activation initially had minimal impact on data volume, its effectiveness in controlling traffic volume increased significantly over time, with the most substantial filtering occurring in the final period. The divergent behavior between flow counts and data volumes

suggests that the firewall became increasingly sophisticated in traffic management, possibly through optimized filtering rules, adaptation to traffic patterns, or enhanced security policies that prioritized data volume control over connection quantity limitations.

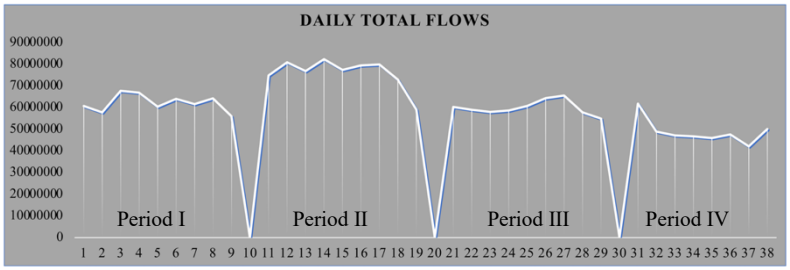

Fig. 7. Daily Total Flows Graph

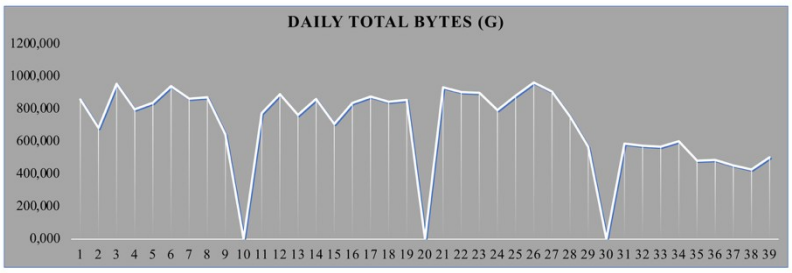

Fig. 8. Daily Total Bytes Graph

Fig. 9 The "DAILY TOTAL PACKETS (G)" chart displays packet volume in Giga packets over 38 periods with consistent phase divisions matching previous graphs, including data cutoffs at points 10, 20, and 30. During firewall filter OFF periods, there was notable variation between period 1 (days 1-9), showing 0.8-1.1 G packets and period 3 (days 21-29), demonstrating substantial growth to 1.2-1.5 G packets. When firewall filter was activated, period 2 (days 11-19) showed increased packet counts of 1.1-1.3 G packets (approximately 20% higher than period 1), while period 4 (days 31-39) dropped significantly to 0.8-1.0 G packets, representing a 30-40% reduction compared to period 3. This pattern reveals an interesting evolution in firewall effectiveness, where initial activation increased packet processing, but later implementation achieved substantial traffic control by reducing both data volume and packet counts simultaneously. The dramatic spike in period 3 followed by the sharp decline in period 4 suggests that the firewall system underwent significant optimization, possibly through improved filtering algorithms, more specific traffic control rules, or adaptive responses to changing network attack patterns, ultimately demonstrating enhanced capability to manage network traffic comprehensively rather than simply tracking connection flows [51], [52].

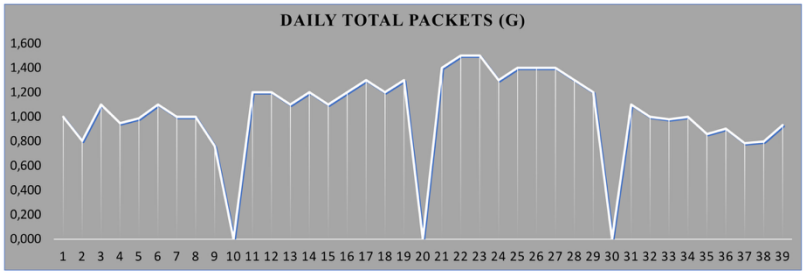

Fig. 9. Daily Total Packets Graph

Fig. 10 The "Daily Average BPS" chart displays network traffic over 39 days, revealing significant patterns related to firewall filter status. During periods 1 and 3 when the firewall filter was OFF, traffic bandwidth showed relatively high and fluctuating values with peaks reaching approximately 80,000-90,000

BPS, indicating that all types of traffic could pass through the network without restrictions or filtering. Conversely, during periods 2 and 4 when the firewall filter was activated (ON), there was a dramatic reduction in traffic bandwidth to approximately 10,000-20,000 BPS, demonstrating that the firewall effectively blocked or limited specific traffic according to configured rules. This pattern indicates that the firewall filter functioned properly in controlling and reducing network traffic load, showing consistent performance across both activation periods with approximately 75-80% traffic reduction when filtering was enabled, confirming the firewall's effectiveness in network traffic management and security implementation .

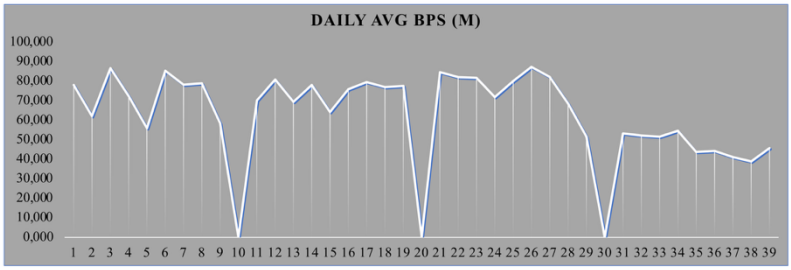

Fig. 10. Daily Average BPS Graph

Fig. 11 The "Daily Average PPS (Packets Per Second)" chart covering 39 days of observation reveals a strong correlation between firewall filter status and packet volume processed in the network. During periods 1 and 3 when the firewall filter was OFF, packets per second showed extremely high values with peaks reaching 16,000-18,000 PPS, indicating that all data packets could pass through the network without filtering or inspection processes that would impede traffic flow. However, during periods 2 and 4, when the firewall filter was activated (ON), there was a significant reduction in PPS to approximately 2,000-4,000 PPS, demonstrating that the firewall effectively performed packet inspection and filtering, allowing only packets meeting security criteria to pass through. This pattern confirms the firewall's effectiveness in controlling packet-based traffic, where filter activation not only reduced bandwidth but also drastically decreased the volume of processed packets by approximately 75-80%, potentially indicating successful blocking of anomalous traffic or attacks that are typically characterized by high packet volumes, thus validating the firewall's capability in both traffic management and security threat mitigation.

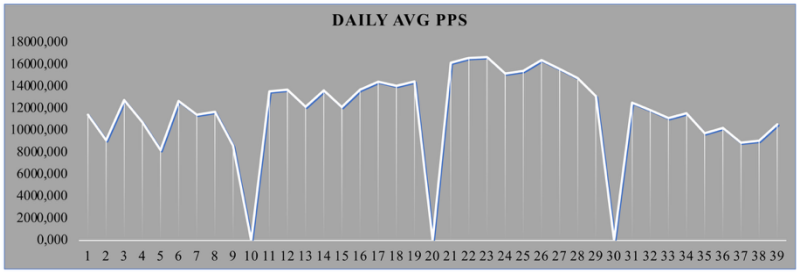

Fig. 11. Daily Total Average PPS Graph

Fig. 12 The "Daily Average BPP (Bytes Per Packet)" chart over 39 days reveals an interesting and different pattern from previous metrics regarding firewall filter activation. During periods 1 and 3, when the firewall filter was OFF, BPP values showed relatively low fluctuations averaging between 100-300 bytes per packet, indicating that network traffic was dominated by small to medium-sized packets, likely including normal traffic and other activities using small packet sizes. Conversely, during periods 2 and 4, when the firewall filter was activated (ON), there was a significant increase in BPP values with peaks reaching 700-800 bytes per packet, demonstrating that although total packet count and bandwidth decreased drastically, packets successfully passing through the firewall tended to be larger. This phenomenon indicates that the firewall filter selectively blocks high-volume traffic with small packets while allowing legitimate traffic that typically has larger packet sizes, resulting in efficient filtering that maintains service quality for business applications requiring large packet data transfers. The 2-3x increase in average packet size during firewall activation

suggests intelligent traffic discrimination, where the system effectively filtered out potentially malicious or unnecessary small-packet traffic while preserving bandwidth for legitimate data-intensive applications.

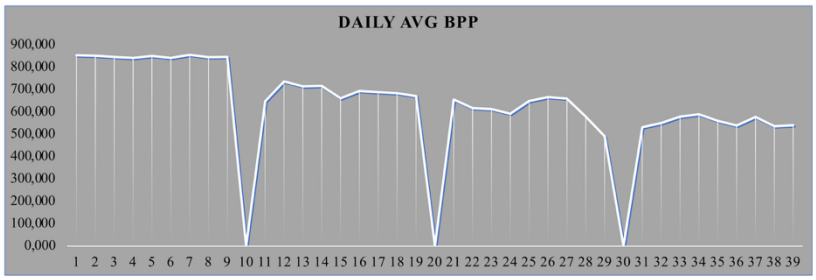

Fig. 12. Daily Total Average BPP Graph

Network Traffic Statistical Analysis

95% Confidence Interval

$$CI = x^{-} \pm t_{\propto/2,df} \times (\frac{s}{\sqrt{n}})$$

x^{-} is sample mean, $t_{\propto/2,df}$ is t-critical value, s is sample standard deviation, n is sample size, df is degrees of freedom (n-1).

Two-Sample t-Test

$$t = \frac{(x_1^{-} - x_2^{-})}{SE_{pooled}}$$

$$SE_{pooled} = S_{pooled} \times \sqrt{(\frac{1}{n_1} + \frac{1}{n_2})}$$

$$S_{pooled=}\sqrt{[((n_1 - 1)s_1^2 + (n_2} - 1)s_2^2)/\ (n_1 + n_2 - 2)]$$

H_0 is $\mu_1 = \mu_2$ (no difference), H_1 is $\mu_1 \neq \mu_2$ (significant difference)

Table 8 Refer to statistical analysis presented in the table, the filter implementation demonstrates mixed effects across different network performance metrics. When the filter is activated (ON state), there is a slight increase in FLOWS from 60.97M to 62.52M, while BYTES decrease substantially from 836.43 to 671.85, and PACKETS show a notable reduction from 1.17 to 1.06. The average bytes per second (AVGBPS) decreases from 74.76 to 60.98 when the filter is active, and similarly, the average bytes per packet (AVGBPP) drops from 730.39 to 622.94. Interestingly, the average packets per second (AVGPPS) shows minimal change from 13.14K to 12.08 K. The wider confidence intervals observed in several metrics when the filter is OFF (particularly in FLOWS and BYTES) suggest greater variability in network behavior without filtering, while the filter appears to provide more consistent performance with tighter confidence bounds, indicating that the filtering mechanism effectively reduces data throughput and packet sizes while maintaining relatively stable flow patterns.

Table 9 The statistical analysis reveals that the filter implementation has statistically significant effects on three key network performance metrics: BYTES, AVGBPS (average bytes per second), and AVGBPP (average bytes per packet), all showing p-values less than 0.05. The filter significantly reduces BYTES by 164.58 units (t-statistic = 3.580), AVGBPS by approximately 0.60 units (t-statistic = 3.198), and AVGBPP by 107.44 units (t-statistic = 3.213), indicating effective data throughput reduction and packet size optimization. While the filter also reduces PACKETS (by 0.11 units) and AVGPPS (by 1.06K units), these changes are not statistically significant ($p > 0.05$), suggesting minimal impact on packet frequency and flow rates. Interestingly, FLOWS shows a non-significant increase of 1,557,024.67 units when the filter is active, indicating that while

the filter allows more connection flows, it effectively constrains the actual data volume and packet characteristics. Overall, the filter demonstrates selective effectiveness, significantly optimizing data transmission efficiency while maintaining network connectivity patterns.

Table 8. 95% Confidence Intervals by Metric

Metric	Filter State	Mean	95% CI Lower	95% CI Upper	Std Dev	n
FLOWS	OFF	60.97M	59.18M	62.75M	3.59M	18
	ON	62.52M	55.26M	69.79M	14.61M	18
BYTES	OFF	836.43	782.68	890.17	108.07	18
	ON	671.85	591.11	752.59	162.35	18
PACKETS	OFF	1.17	1.06	1.29	0.23	18
	ON	01.06	0.98	1.14	0.16	18
AVGBPS	OFF	74.76	69.38	80.13	10.81	18
	ON	60.98	53.66	68.31	14.73	18
AVGPPS	OFF	13.14K	11.77K	14.51K	2.76K	18
	ON	12.08K	11.19K	12.96K	1.78K	18
AVGBPP	OFF	730.39	669.33	791.45	122.77	18
	ON	622.94	587.60	658.29	71.07	18

Table 9. Statistical Significance Testing α =0.05)

Metric	Mean Difference (OFF - ON)	t-Statistic	p-value	Significant?	Effect
FLOWS	-1557024.67	-0.439	> 0.05	NO	Filter increases metric
BYTES	164.58.00	3.580	< 0.05	YES	Filter reduces metric
PACKETS	00.11	1.640	> 0.05	NO	Filter reduces metric
AVGBPS	0,595138889	3.198	< 0.05	YES	Filter reduces metric
AVGPPS	1.06K	1.377	> 0.05	NO	Filter reduces metric
AVGBPP	107.44.00	3.213	< 0.05	YES	Filter reduces metric

Table 10 The periodic network traffic analysis table reveals distinct patterns in firewall filter performance across four operational phases, demonstrating the evolving effectiveness of traffic control mechanisms. During the first transition from FILTER OFF to ON, total flows increased by 22% (from 62M to 76M) while maintaining similar data volumes (828G to 823G) and bandwidth (73M to 75M bps), but with a 26% increase in packet processing (0.97G to 1.20G packets) and packet rates (10.7K to 13.5K pps), suggesting initial firewall activation generated additional connection tracking overhead. However, the second transition shows dramatically different behavior, where FILTER ON implementation achieved substantial traffic reduction across all metrics: flows decreased by 18% (from 60M to 49M), data volume dropped by 38% (from 845G to 520G), packets reduced by 33% (from 1.38G to 0.93G), bandwidth fell by 38% (from 77M to 47M bps), and packet rates decreased by 32% (from 15.5K to 10.6K pps). Notably, average bytes per packet (bpp) consistently decreased when filtering was active, from 847 to 690 in the first phase and from 613 to 556 in the second phase, indicating that the firewall increasingly targeted smaller packet traffic while allowing larger, potentially more legitimate data transfers to pass through, demonstrating sophisticated traffic discrimination capabilities that evolved to become more restrictive and effective over time.

Fig. 13 The Periodic Total Flows chart displaying aggregate data across 4 periods reveals significant firewall filter impact on network data flows. During periods 1 and 3 with firewall filter OFF, total flows reached extremely high values of 62,085,056 and 59,846,847 respectively, indicating massive network activity where all connection types could form unrestricted, potentially including anomalous traffic, attacks, or scanning activities generating numerous flow connections. Conversely, when firewall filter was activated (ON) in periods 2 and 4, flows dropped to 75,872,845 and dramatically decreased to 49,173,108 respectively, demonstrating the firewall's effectiveness in blocking unwanted connections and controlling active network sessions. The gradual reduction from period 2 to period 4 with firewall active indicates a learning curve or increasingly strict configuration adjustments, where the firewall became more efficient at identifying and blocking suspicious traffic patterns, resulting in a more secure network environment with controlled and legitimate flow connections.

Fig. 14 The Periodic Total Bytes chart showing bandwidth consumption in Gigabytes across 4 periods demonstrates consistent firewall filter effectiveness in controlling data volume passing through the network. During periods 1 and 3 with firewall filter OFF, total bytes reached high values of 827,989 GB and 844,867 GB,, respectively, indicating unrestricted data flow, including potential unnecessary transfers, malicious activity, or bandwidth abuse, consuming excessive network capacity. When the firewall filter was activated (ON) in periods 2 and 4, while period 2 remained relatively high at 823,256 GB, period 4 showed a significant reduction to 520,444 GB, demonstrating the firewall's gradual improvement in blocking unwanted traffic and

optimizing bandwidth usage. The dramatic 38% decrease in period 4 indicates that firewall filtering not only reduced connection counts and packets but also substantially decreased overall bandwidth consumption, creating significant network efficiency while maintaining legitimate traffic for normal business operations.

Table 10. Periodic data- FILTER OFF and ON

	PERIODIC Total Flows	PERIODIC Total Bytes (G)	PERIODIC Total Packets (G)	PERIODIC Avg bps (M)	PERIODIC Avg pps	PERIODIC Avg bpp
FILTER OFF	62085056	827,989	0,967	72,878	10742,778	847,444
FILTER ON	75872845	823,256	1,200	74,722	13535,222	689,889
FILTER OFF	59846847	844,867	1,378	76,633	15536,444	613,333
FILTER ON	49173108	520,444	0,928	47,244	10616,333	556,000

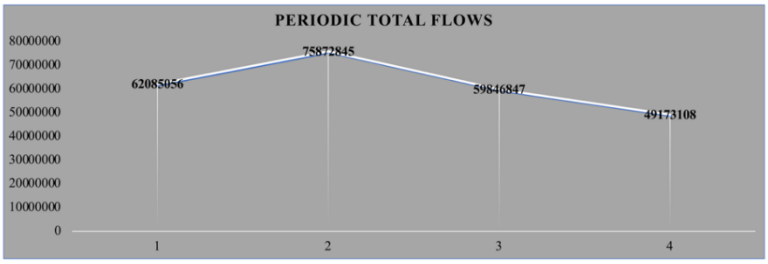

Fig. 13. Periodic Total Flows Graph Fluctuation

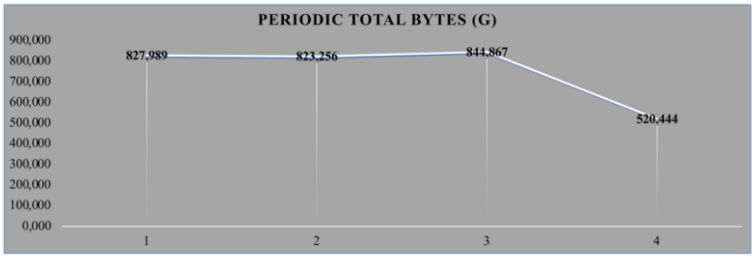

Fig. 14. Periodic Total Bytes Graph Fluctuation

Fig. 15 The graph shows packet traffic over 4 periods with the firewall turned off and on alternately. When the firewall was off (periods 1 and 3), packet volumes were 0.967 and 1.378 Gigapackets, with period 3 showing the highest traffic, including unwanted packets. When the firewall was on (periods 2 and 4), there was initially higher traffic at 1.200 Gigapackets in period 2 as the firewall activated, but by period 4, it dropped to the lowest level at 0.928 Gigapackets. This proves the firewall effectively blocks unwanted traffic and creates a more stable network with only legitimate traffic remaining.

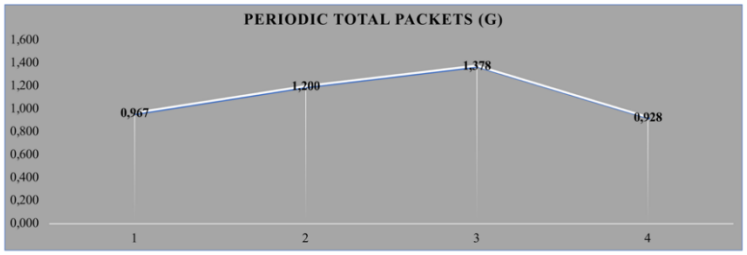

Fig. 15. Periodic Total Packets Graph Fluctuation

Fig. 16 The Periodic Average BPS graph shows bandwidth usage in Mega BPS across 4 periods, revealing how the firewall optimizes network bandwidth. When the firewall was off (periods 1 and 3), bandwidth usage was high at 72.878 MBPS and 76.633 MBPS, respectively, with period 3 reaching the peak, indicating unrestricted traffic consumption, including potential bandwidth abuse and inefficient data transfers. When the firewall was on (periods 2 and 4), although period 2 remained relatively high at 74.722 MBPS, period 4 dropped dramatically to 47.244 MBPS - about 38% lower than previous periods. This significant reduction shows the firewall not only reduced connections and packets but also effectively optimized bandwidth usage by blocking unproductive traffic, creating substantial network efficiency while maintaining service quality for legitimate business applications.

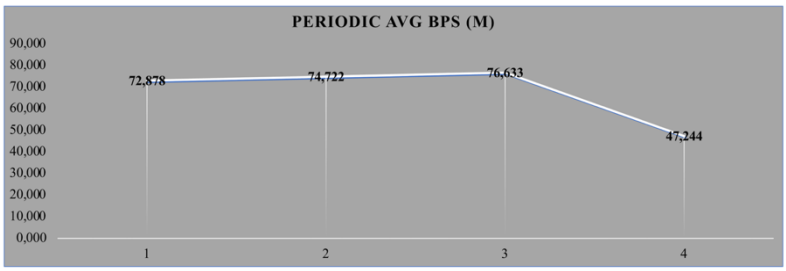

Fig. 16. Periodic Average BPS Graph Fluctuation

Fig. 17 The Periodic Average PPS graph shows packets per second across 4 periods, clearly demonstrating the firewall's impact on packet processing volume. When the firewall was off (periods 1 and 3), average PPS was 10,742.778 and peaked at 15,536.444 PPS in period 3, indicating significant network activity spikes with very high packet volumes, possibly including traffic anomalies, flooding attacks, or scanning activities generating large packet bursts. When the firewall was on (periods 2 and 4), although period 2 showed an increase to 13,535.222 PPS (likely due to initial system response), period 4 dropped dramatically to 10,616.333 PPS - nearly equivalent to period 1 but under controlled conditions. This confirms the firewall's effectiveness in controlling packet rates, where after a learning and optimization phase, it successfully stabilized PPS volume at safe and controlled levels, protecting the network from high-volume packet attacks while maintaining adequate throughput for normal operations

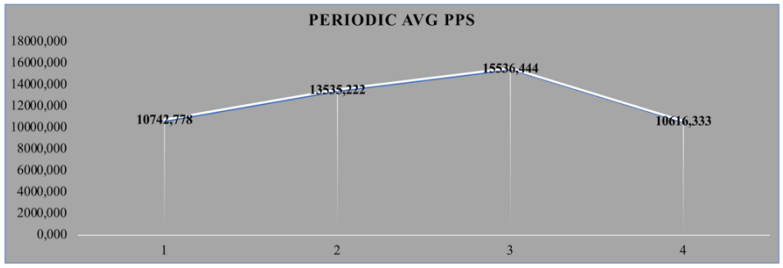

Fig. 17. Periodic Average PPS Graph Fluctuation

Fig. 18 The Periodic Average BPP graph shows bytes per packet across 4 periods, revealing a consistent declining pattern related to how the firewall affects packet size characteristics. When the firewall was off (periods 1 and 3), average BPP was high at 847.444 bytes and 613.333 bytes per packet respectively, with period 1 reaching the highest value, indicating network traffic dominated by large packets possibly including legitimate data transfers, file sharing, or applications requiring large payloads. When the firewall was on (periods 2 and 4), there was a progressive decrease in average packet size to 689.889 bytes in period 2 and further down to 556.000 bytes in period 4. This continuous BPP decline shows the firewall selectively blocks or limits large packets that may be considered suspicious or violate security policies, resulting in traffic dominated by smaller but safer and more controlled packets, creating a more efficient and secure network profile. The Periodic Average BPP graph shows bytes per packet across 4 periods, revealing a consistent declining pattern related to how the firewall affects packet size characteristics. When the firewall was off (periods 1 and 3), average BPP was high at 847.444 bytes and 613.333 bytes per packet respectively, with

period 1 reaching the highest value, indicating network traffic dominated by large packets possibly including legitimate data transfers, file sharing, or applications requiring large payloads. When the firewall was on (periods 2 and 4), there was a progressive decrease in average packet size to 689.889 bytes in period 2 and further down to 556.000 bytes in period 4. This continuous BPP decline shows the firewall selectively blocks or limits large packets that may be considered suspicious or violate security policies, resulting in traffic dominated by smaller but safer and more controlled packets, creating a more efficient and secure network profile.

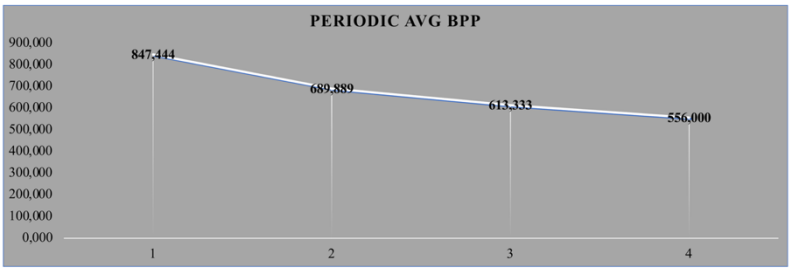

Fig. 18. Periodic Average BPP Graph Fluctuation

Table 11 presents a comparative analysis of network traffic data between two scenarios: when the filter was off and when it was on. The figures reveal that activating the filter led to an increase in total flows by 2.49%, while other metrics showed a decrease. Notably, total bytes dropped by 24.50%, total packets by 10.15%, total average bits per second by 22.58%, total average packets per second by 8.81%, and total average bytes per packet by 17.25%. This suggests that while the number of total flows increased slightly, the overall data volume and transmission rate were significantly reduced when the filter was applied.

Table 11. Total data - FILTER OFF and ON with Increase / Decrease Value

	TOTAL Flows	TOTAL Bytes (G)	TOTAL Packets (G)	TOTAL Avg bps (M)	TOTAL Avg pps	TOTAL Avg bpp
FILTER OFF	60965952	836,428	1,172	74,756	13139,611	730,389
FILTER ON	62522976	671,850	1,064	60,983	12075,778	622,944
INCREASE/DECREASE OFF to ON	2,49%	-24,50%	-10,15%	-22,58%	-8,81%	-17,25%

Here's an analysis of the total data above, focusing on changes in network performance when the firewall is on (filter on) compared to when it is turned off (filter off):

Fig. 19 Total Flows: Filter Off: 60,965,952, Filter On: 62,522,976, Change: +2.49%. Although the total flows increase slightly when the firewall is activated, this suggests that the firewall may let most of the connections through, but does not significantly increase the number of connections.

Fig. 20 Total Bytes (G): Filter Off: 836,428, Filter On: 671,850, Change: -24.50. There is a significant drop in the total number of bytes when the firewall is activated. This could indicate that a large amount of data is being rejected or restricted by a firewall policy, which may serve to prevent unwanted or malicious data transfers.

Fig. 21 Total Packets (G): Filter Off: 1,172, Filter On: 1,064, Change: -10.15%. The decrease in the number of packets indicates that the firewall may have prevented some packets from being detected as insecure data packets. This shows the success of firewalls in controlling unwanted traffic, but it can also impact network performance if important packets are also blocked.

Fig. 22 Avg bps (M): Filter Off: 74,756, Filter On: 60,983, Change: -22.58%. When the firewall is enabled, the average bandwidth (bps) used is significantly reduced. This decrease may reflect a reduction in the flow of data that is successfully forwarded, possibly due to blocking large packets or unwanted data.

Fig. 23 Avg pps; Filter Off: 13,139,611, Filter On: 12,075,778, Change: -8.81%. The average packets per second (PPS) transmitted also decreased, indicating that with the firewall enabled, the average number of packets transferred decreased. This can contribute to a decrease in overall connection speed.

Fig. 24 Avg bpp: Filter Off: 730,389, Filter On: 622,944, Change: -17.25. The decrease in the average byte per packet indicates that with the firewall on, more small packets are successfully traversed, probably because large packets are more likely to be blocked. This can lead to a decrease in data transmission efficiency.

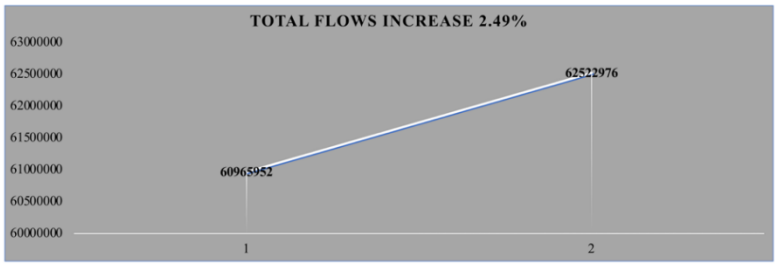

Fig. 19. Total Flows Graph Increase

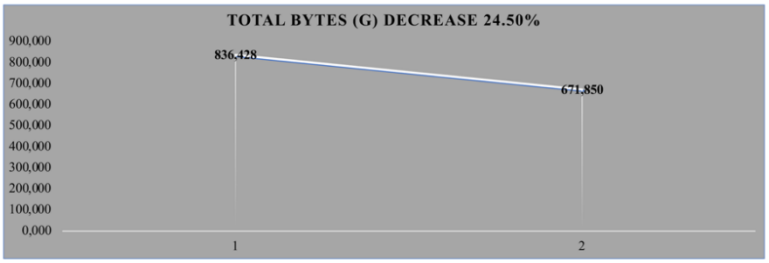

Fig. 20. Total Bytes Graph Decrease

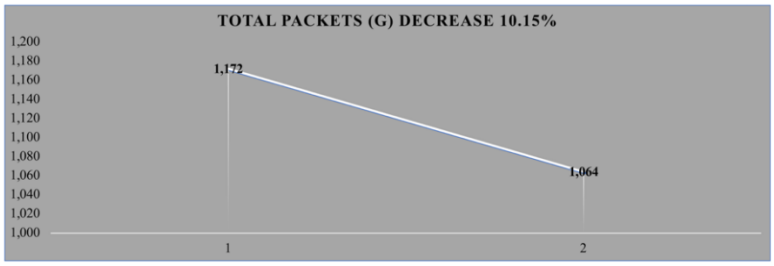

Fig. 21. Total Packets Graph Decrease

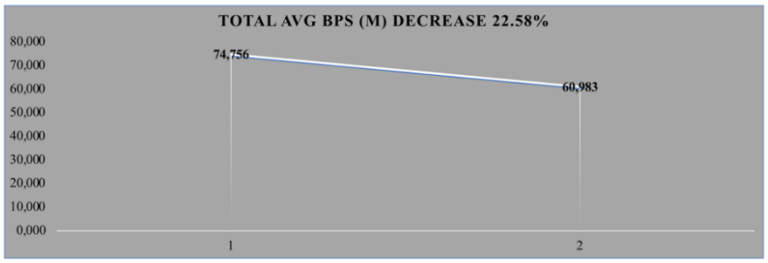

Fig. 22. Total Average BPS Graph Decrease

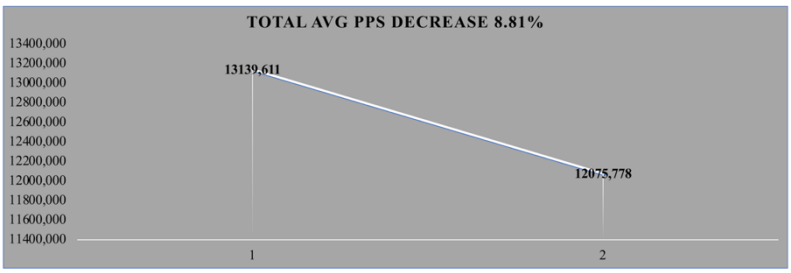

Fig. 23. Total Average PPS Graph Decrease

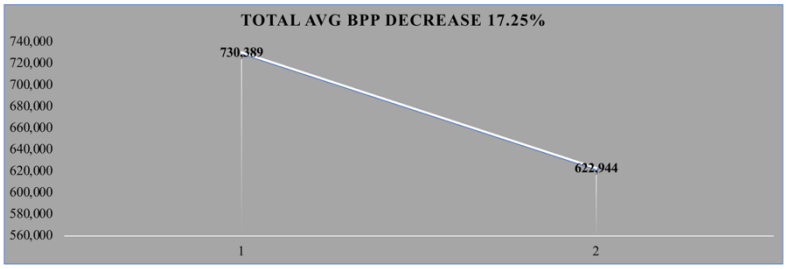

Fig. 24. Total Average BPP Graph Decrease

Compared to similar studies, our findings demonstrate both similarities and differences in the effectiveness of blacklist-based domain filtering. Cozza et al. [34] reported a 12-18% reduction in malicious traffic using DNS-based filtering, which is lower than our observed 24.5% reduction in total bytes. This difference may be attributed to our implementation at the ISP level rather than the endpoint level. Conversely, Pitafi et al. [36] achieved a 30% reduction in malicious traffic but required significantly more computational resources than our approach, making it less suitable for resource-constrained environments. Our approach offers a better balance between effectiveness and resource efficiency compared to these previous methods.

The observed 2.49% increase in total flows alongside the 24.5% reduction in bytes transferred represents an important trade-off in the implementation of malicious domain filtering. While the increased flows indicate additional connection attempts (likely retry mechanisms when connections are blocked), the substantial reduction in data transfer demonstrates the effectiveness of the filtering system in preventing potentially malicious content from reaching client systems. For ISPs, this trade-off is generally advantageous, as the marginal increase in connection processing is outweighed by the significant reduction in potentially harmful data transmission and the associated security benefits. However, in extremely high-traffic environments, the additional connection processing should be considered when dimensioning router resources.

4. CONCLUSION

The study's results demonstrate a significant impact from implementing malicious domain filtering firewalls. Regarding traffic flow, there was a 2.49% increase in total flow, attributed to the retry connection mechanism when a domain was blocked. When a user attempts to access a malicious domain and is blocked by a firewall, the client system automatically performs several reconnection attempts, which are logged as new flow. However, the effect of this retry connection was not significant on bandwidth, as filtering reduced total bytes by 24.5% and total packets by 10.5%, with an average bandwidth decrease (bps) of 22.58% and a packet rate decrease (pps) of 8.81%. The effectiveness of filtering is evident from the detection of 1,090 IP addresses of users who attempted to access malicious domains, with 1,919 malicious IP addresses successfully blocked. These findings confirm that the filtering method enhances user security and optimizes bandwidth usage by eliminating unwanted traffic. Additionally, this method facilitates the implementation of existing products used by ISPs. It is advisable to combine this malicious domain filtering with various layered security strategies to achieve optimal results.

Despite these promising results, several limitations should be acknowledged. First, our study was conducted with a single ISP in a specific regional context, which may limit generalizability to ISPs with significantly different traffic patterns or user behaviors. Second, our reliance on static blacklists, while effective against known threats, does not address zero-day attacks or rapidly evolving threats that may not yet be included in public blacklists. Third, our evaluation focused primarily on technical performance metrics rather than user experience, which could be affected by factors beyond the scope of our measurement framework. This approach does not account for zero-day threats, which may not be present on the existing blacklist. Future research should focus on three key areas: (1) Integration of machine learning techniques with blacklist-based filtering to enable real-time detection of previously unknown malicious domains based on behavioral patterns; (2) Development of automated, adaptive blacklist updating mechanisms that can respond to emerging threats with minimal human intervention; and (3) Expansion of the evaluation framework to include diverse ISP environments and user populations to enhance generalizability. These directions would address the current limitations of static blacklist approaches while building on the demonstrated effectiveness of the basic filtering mechanism. This study has made two significant contributions to the field of cybersecurity for ISPs: first, demonstrating that effective malicious domain filtering can be implemented with minimal additional infrastructure using existing router capabilities; and second, providing quantitative evidence of the specific

security and performance impacts of such filtering, enabling ISPs to make informed decisions about implementation. These contributions directly address the practical challenges faced by growing ISPs with limited resources while advancing the understanding of cybersecurity implementation trade-offs.

REFERENCES

[1] Y. Shaengchart and T. Kraiwanit, "Starlink satellite project impact on the Internet provider service in emerging economies," *Research in Globalization*, vol. 6, Jun. 2023, https://doi.org/10.1016/j.resglo.2023.100132.
[2] M. Zeng, J. Du, X. Zhu, and X. Deng, "Does internet use drive rural household savings? Evidence from 7825 farmer households in rural China," *Financ Res Lett*, vol. 57, Nov. 2023, https://doi.org/10.1016/j.frl.2023.104275.
[3] P. Babari, M. Hielscher, P. A. Edelsbrunner, M. Conti, B. D. Honegger, and E. Marinus, "A literature review of children's and youth's conceptions of the internet," *Elsevier B.V.,* 2023, https://doi.org/10.1016/j.ijcci.2023.100595.
[4] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith, and S. Creese, "A system to calculate cyber-value-at-risk," *Comput Secur*, vol. 113, Feb. 2022, https://doi.org/10.1016/j.cose.2021.102545.
[5] P. H. Meland, D. A. Nesheim, K. Bernsmed, and G. Sindre, "Assessing cyber threats for storyless systems," *Journal of Information Security and Applications*, vol. 64, Feb. 2022, https://doi.org/10.1016/j.jisa.2021.103050.
[6] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, https://doi.org/10.1016/j.egyr.2021.08.126.
[7] Y. Takefuji, "Case report on enormous economic losses caused by fraud from Japan to the world," *Journal of Economic Criminology*, vol. 1, p. 100003, Sep. 2023, https://doi.org/10.1016/j.jeconc.2023.100003.
[8] M. Ghosh, D. Ghosh, R. Halder, and J. Chandra, "Investigating the impact of structural and temporal behaviors in Ethereum phishing users detection," *Blockchain: Research and Applications*, vol. 4, no. 4, Dec. 2023, https://doi.org/10.1016/j.bcra.2023.100153.
[9] H. Spencer, W. Wang, R. Sun, and M. Xue, "Dissecting Malware in the Wild," *ACM International Conference Proceeding Series*, pp. 56–64, 2022, https://doi.org/10.1145/3511616.3513099.
[10] S. H. Ahammad *et al.*, "Phishing URL detection using machine learning methods," *Advances in Engineering Software*, vol. 173, Nov. 2022, https://doi.org/10.1016/j.advengsoft.2022.103288.
[11] A. M. Manasrah, T. Khdour, and R. Freehat, "DGA-based botnets detection using DNS traffic mining," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 2045–2061, May 2022, https://doi.org/10.1016/j.jksuci.2022.03.001.
[12] X. Shen, X. Zhang, and Y. Chen, "Deep Learning Powered Adversarial Sample Attack Approach for Security Detection of DGA Domain Name in Cyber Physical Systems," *IEEE Wirel Commun*, vol. 29, no. 2, pp. 16–21, Apr. 2022, https://doi.org/10.1109/MWC.001.2100247.
[13] K. Hausken, "Cyber resilience in firms, organizations and societies," *Elsevier B.V.*, 2020, https://doi.org/10.1016/j.iot.2020.100204.
[14] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput Secur*, vol. 120, Sep. 2022, https://doi.org/10.1016/j.cose.2022.102820.
[15] A. Gusev, "Domestic private banking solutions can be quite successful as an effective protection against whaling-style cyber attacks which are used as a basis for more complex targeted phishing," in *Procedia Computer Science*, pp. 391–399, 2022, https://doi.org/10.1016/j.procs.2022.11.083.
[16] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput Secur*, vol. 105, Jun. 2021, https://doi.org/10.1016/j.cose.2021.102239.
[17] H. J. Motulsky, T. Head, and P. B. S. Clarke, "Analyzing lognormal data: A nonmathematical practical guide," *Elsevier Inc.*, 2025, https://doi.org/10.1016/j.pharmr.2025.100049.
[18] F. P. B. Mota and I. Cilento, "Competence for internet use: Integrating knowledge, skills, and attitudes," *Computers and Education Open*, vol. 1, p. 100015, Dec. 2020, https://doi.org/10.1016/j.caeo.2020.100015.
[19] H. Ismail, F. Febiyanto, Kevin, and J. V. Moniaga, "Methods to prevent privacy violations on the internet on the personal level in Indonesia," in *Procedia Computer Science*, pp. 650–654, 2022, https://doi.org/10.1016/j.procs.2022.12.180.
[20] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digital Communications and Networks*, vol. 8, no. 4, pp. 422–435, Aug. 2022, https://doi.org/10.1016/j.dcan.2021.07.006.
[21] E. K. Szczepaniuk and H. Szczepaniuk, "Analysis of cybersecurity competencies: Recommendations for telecommunications policy," *Telecomm Policy*, vol. 46, no. 3, Apr. 2022, https://doi.org/10.1016/j.telpol.2021.102282.
[22] A. G. Martín, M. Beltrán, A. Fernández-Isabel, and I. Martín de Diego, "An approach to detect user behaviour anomalies within identity federations," *Comput Secur*, vol. 108, Sep. 2021, https://doi.org/10.1016/j.cose.2021.102356.
[23] V. Gkioulos and N. Chowdhury, "Cyber security training for critical infrastructure protection: A literature review," *Elsevier Ireland Ltd.*, 2021, https://doi.org/10.1016/j.cosrev.2021.100361.
[24] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess Microsyst*, vol. 77, Sep. 2020, https://doi.org/10.1016/j.micpro.2020.103201.

[25] H. Ho, R. Ko, and L. Mazerolle, "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review," *Comput Secur*, vol. 115, Apr. 2022, https://doi.org/10.1016/j.cose.2022.102611.
[26] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "A forensics and compliance auditing framework for critical infrastructure protection," *International Journal of Critical Infrastructure Protection*, vol. 42, Sep. 2023, https://doi.org/10.1016/j.ijcip.2023.100613.
[27] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," *Elsevier Ltd*, 2023, https://doi.org/10.1016/j.cose.2023.103123.
[28] Y. Zeng, "AI Empowers Security Threats and Strategies for Cyber Attacks," in *Procedia Computer Science*, pp. 170–175, 2022, https://doi.org/10.1016/j.procs.2022.10.025.
[29] C. Marques, S. Malta, and J. P. Magalhães, "DNS dataset for malicious domains detection," *Data Brief*, vol. 38, Oct. 2021, https://doi.org/10.1016/j.dib.2021.107342.
[30] N. Miloslavskaya, D. Stodelov, M. Malakhov, and A. Marachyova, "Security Architecture of Network Security Centers as Part of Modern Intranets," in *Procedia Computer Science*, pp. 58–63, 2022, https://doi.org/10.1016/j.procs.2022.11.038.
[31] K. Yoshida, K. Fujiwara, A. Sato, and S. Sannomiya, "Cardinality Analysis to Classify Malicious Domain Names," in *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, pp. 826–832, 2020, https://doi.org/10.1109/COMPSAC48688.2020.0-161.
[32] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *KeAi Communications Co,* 2024, https://doi.org/10.1016/j.csa.2023.100031.
[33] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," *Communications Co,* 2024, https://doi.org/10.1016/j.iotcps.2023.09.003.
[34] A. N. Kia, F. Murphy, B. Sheehan, and D. Shannon, "A cyber risk prediction model using common vulnerabilities and exposures," *Expert Syst Appl*, vol. 237, Mar. 2024, https://doi.org/10.1016/j.eswa.2023.121599.
[35] F. Rustam and A. D. Jurcut, "Malicious traffic detection in multi-environment networks using novel S-DATE and PSO-D-SEM approaches," *Comput Secur*, vol. 136, Jan. 2024, https://doi.org/10.1016/j.cose.2023.103564.
[36] T. Kwon *et al.*, "How to decentralize the internet: A focus on data consolidation and user privacy," *Elsevier B.V,* 2023, https://doi.org/10.1016/j.comnet.2023.109911.
[37] M. Benyahya, A. Collen, S. Kechagia, and N. A. Nijdam, "Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments," *Comput Secur*, vol. 122, Nov. 2022, https://doi.org/10.1016/j.cose.2022.102904.
[38] L. Böck, E. Vasilomanolakis, J. H. Wolf, and M. Mühlhäuser, "Autonomously detecting sensors in fully distributed botnets," *Comput Secur*, vol. 83, pp. 1–13, Jun. 2019, https://doi.org/10.1016/j.cose.2019.01.004.
[39] S. O'Shaughnessy and F. Breitinger, "Malware family classification via efficient Huffman features," *Forensic Science International: Digital Investigation*, vol. 37, Jul. 2021, https://doi.org/10.1016/j.fsidi.2021.301192.
[40] C. Marques, S. Malta, and J. P. Magalhães, "DNS dataset for malicious domains detection," *Data Brief*, vol. 38, Oct. 2021, https://doi.org/10.1016/j.dib.2021.107342.
[41] S. Pitafi, T. Anwar, I. D. M. Widia, B. Yimwadsana, and S. Pitafi, "Revolutionizing Perimeter Intrusion Detection: A Machine Learning-Driven Approach with Curated Dataset Generation for Enhanced Security," *IEEE Access*, vol. 11, pp. 106954–106966, 2023, https://doi.org/10.1109/ACCESS.2023.3318600.
[42] M. P. Karpowicz, "Adaptive tuning of network traffic policing mechanisms for DDoS attack mitigation systems," *Eur J Control*, vol. 61, pp. 101–118, Sep. 2021, https://doi.org/10.1016/j.ejcon.2021.07.001.
[43] O. Van Der Toorn, M. Müller, S. Dickinson, C. Hesselman, A. Sperotto, and R. Van Rijswijk-Deij, "Addressing the challenges of modern DNS a comprehensive tutorial," *Elsevier Ireland Ltd.*, 2022, https://doi.org/10.1016/j.cosrev.2022.100469.
[44] I. Dutt, S. Borah, and I. K. Maitra, "Multiple Immune-based Approaches for Network Traffic Analysis," in *Procedia Computer Science*, pp. 2111–2123, 2020, https://doi.org/10.1016/j.procs.2020.03.259.
[45] P. Jurkiewicz, G. Rzym, and P. Boryło, "Flow length and size distributions in campus Internet traffic," *Comput Commun*, vol. 167, pp. 15–30, Feb. 2021, https://doi.org/10.1016/j.comcom.2020.12.016.
[46] P. Jurkiewicz, "flow-models: A framework for analysis and modeling of IP network flows," *SoftwareX*, vol. 17, Jan. 2022, https://doi.org/10.1016/j.softx.2021.100929.
[47] L. Yu *et al.*, "PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection," *Computer Networks*, vol. 194, Jul. 2021, https://doi.org/10.1016/j.comnet.2021.108117.
[48] S. R. Stock and F. De Carlo, "Meta-data for absorption tomography measurements," *Tomography of Materials and Structures*, vol. 3, p. 100015, Sep. 2023, https://doi.org/10.1016/j.tmater.2023.100015.
[49] S. Jacob, Y. Qiao, Y. Ye, and B. Lee, "Anomalous distributed traffic: Detecting cyber security attacks amongst microservices using graph convolutional networks," *Comput Secur*, vol. 118, Jul. 2022, https://doi.org/10.1016/j.cose.2022.102728.
[50] D. Vake, J. Vičič, and A. Tošić, "Hive: A secure, scalable framework for distributed Ollama inference," *SoftwareX*, vol. 30, May 2025, https://doi.org/10.1016/j.softx.2025.102183.
[51] J. A. Morales and Y. Cai, "Analyzing temporal graphs of malware distribution networks," *Array*, vol. 14, Jul. 2022, https://doi.org/10.1016/j.array.2022.100174.
[52] I. El Alaoui and Y. Gahi, "Network security strategies in big data context," in *Procedia Computer Science*, pp. 730–736, 2020, https://doi.org/10.1016/j.procs.2020.07.108.

BIOGRAPHY OF AUTHORS

Muhti Subiyantoro, Completed undergraduate studies at Muhammadiyah of Malang University–UMM in 1999 in the field of Electronic Engineering. Currently active as a professional instructor with a certification issued by MikroTik and Ubquiti in the field of computer and Wireless Networking. All activity under PT. Spectrum Indowibawa, Infrastructure Networks Specialist. The author's area of interest is wireless and wired networking, Fiber Optic and embedded systems. Email: 21917014@students.uii.ac.id.

Mukhammad Andri Setiawan is an assistant professor at Universitas Islam Indonesia. He received his Ph.D. from the University of Queensland, Australia. Currently, he serves as Chief Information Officer at Universitas Islam Indonesia and as head of training and human resources development at Indonesia Network Information Center (IDNIC), the National Internet Registry of the Republic of Indonesia. His main research interests are in the area of Information Systems, such as business process management and improvement, organizational change through the information system, IT governance, IT security, and research area in the development of the Internet of Things. Email: andri@uii.ac.id; ORCID: 0000-0002-2461-6104.